Shushane & co   WAVESTONE

FRANCE & ISRAEL
CYBER INNOVATION WATCH

INSIDER THREAT: SECURE YOUR CRITICAL DATA AND IT INFRASTRUCTURE

The cyber risk posed to an organization because of negligence or intentional attacks of "insiders" (employees or third parties working inside of the same organisation) is dubbed as « insider threat ». Today's data tends to prove that these insiders' threats grow at an exponential rate, and so does their cost.

Insider Threat: Today's main issue for CISOs

Since they have to deal with a growing number of critical infrastructures or devices with access to sensitive data and a growing number of users with excessive access privileges, organizations are increasingly vulnerable to insider threat. Hence the urgency CISOs have to mitigate a threat representing a massive share of attacks and financial damages.

Measure the risks

Though aware of the risks, companies' security programmes often fall short. Therefore, businesses should first precisely measure the risks they are facing as this is required to properly understand and appreciate them before pursuing larger plans. Since cyber priorities are now competing, quantifying cyber risks and the return of investment of prevention programmes is a prerequisite. Intending to help CISOs initiating this necessary review to define a roadmap of cybersecurity actions and beckon executive attention, **Citalid** elaborated a new approach. By mapping the array of insider risks companies are facing and by demonstrating the combination of security measures and in-depth cultural changes mandatory to tackle insider threat, organizations can yield ambitious results.

$350,000

AVALANCHE

**AVERAGE COST OF A
SINGLE MALICIOUS
INSIDER ATTACK**

(not taking into account the
reputation risks and other side
effects costs)

Source: *InCyber,* 2018 White paper.

Identify hotspots through prediction

Aware of the risks they are facing and the measures they should implement, businesses should then identify insiders eager to consider company's assets thefts or leaks. The most recent examples of insider attacks demonstrate that insiders become malicious gradually. Being able to identify months or years of warning signs to prevent insider events upfront instead of reacting afterwards can avoid substantial damages. Common barriers to predict cyber risks caused by insiders are the huge volume of false positives and the perception of privacy invasion. **InCyber** however, developed InCyber On-Prem, which supplies True Prediction of Insider Threats (TPIT), helping companies predict insider attacks through warning signs with nearly zero false positive rate and full compliance to privacy regulations.

Strengthen segmentation

Today's businesses increasingly rely on IT assets like databases, file servers, cloud applications or mobile devices. Therefore, companies have to protect the access risky insiders possess and the most vulnerable data owned like intellectual property, confidential business information or passwords. The U.S. Department of Homeland Security argues that "insider threats (…) are often carried out through abusing access rights". Hence is Identity and Access Management (IAM) solutions a priority to deter insider threats. Yet, if IAM offers a strong barrier against carelessness, when it comes to malicious insiders willing to harm their organization by stealing or leaking vulnerable data, most solutions lack strong authentication

principles. Using behavioural metrics and biometric information like key strokes patterns to encourage organizations strengthen them, **Azguard** ensures that the segmentation is respected.

Protect payments

Over the last years, critical activities like payments' management have been gathered in the hands of privileged insiders and have become harder to trace and secure for global companies. In 2018, an estimated 82% of corporates were victims of payment frauds, and attacks emerged from within the organization in more than half of the cases. Hence should global companies managing suppliers and accounts consider a complete anti-fraud solution. **NsKnox**, offers a real time corporate payment protection named TxAuthority. As frauds have grown exponentially, helping companies prevent false invoices, false billing schemes from malicious insiders or "CEO impersonation frauds" exploiting negligent managers is essential to avoid sizeable financial wounds.

Shifting focus on detection and incident response

Detecting insider attacks is much more difficult than outsider ones, as legitimate access are used. Monitoring of key IT infrastructures and resources must adapt and corporates should adopt innovative network and data security solutions. Since influence over insiders or negligence can initiate espionage of increasingly sensitive data, global companies such as industrial big businesses have to further protect the access to their databases. Today, operators and IT administrators can easily set a VPN from a hidden location to

the company's most valuable resources and define a legitimate source address to access the data. To avoid such a scenario and strengthen network security, **Embedded Solutions** commercialise BitNetSentry.

Using authorized access, insiders or partners can also cause data leaks. Breaches result in a massive negative impact, both financially and on the company's customer base. Hence should corporates consider implementing data-centric solutions that allow to tightly control access and to trace misuses. **WaToo** uses watermarking to conceal tags within documents that allow companies to identify the source of a leak or of a theft.

Organizations that have accepted the surging prevalence of insider threats are now shifting their focus on detection and comprehensive incident response plans and extending CISOs' prerogatives.

Conclusion

Today's studies tend to prove that Insider Threat is one the largest issue in cybersecurity. However, barriers to programmes combating it remain strong. Among them, lack of expertise, suitable technology and budget or the growing measures ensuring insider privacy are often mentioned. Using innovative solutions developed by start-ups can help organizations overcome these obstacles at a low cost and with a very high measurable return on investment.

50%
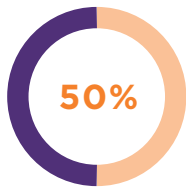
of **SECURITY BREACHES** are caused by trusted insiders[2]

74%
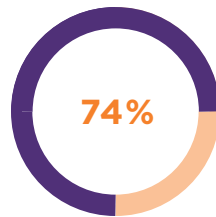
of cybersecurity professionals indicate that **"INSIDER THREATS ARE THE BIGGEST SECURITY ISSUE TODAY"**[1]

56%
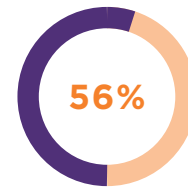
of CISOs consider that **"INSIDER ATTACKS HAVE BECOME MORE FREQUENT IN THEIR ORGANIZATION OVER THE PAST 12 MONTHS"**[1]

Sources:
1. *InCyber,* 2018 White paper.
2. *McKinsey study based on the VERIS Community Database,* 2018.

CISOs prerogatives should widen

Since they have the better understanding of the insiders' prerogatives and already play a transversal support role in the organisation, CISOs have the opportunity to play a key role in fighting insider threats. Indeed, in addition to pursuing mitigation of threats and associated damages, CISOs can raise awareness on these specific cybersecurity risks, be the coordinator for recommending and implementing innovative solutions, help the different departments that are involved in fighting risks to collaborate in a synergic way, and increase in-depth cultural change.

Innovative Israeli and French start-ups can help companies address insider threats with new weapons

Citalid

- Created in 2016
- Located in Paris
- 2 employees (6 in September)
- Field of expertise : Threat Intelligence

Citalid helps managers establish the adequate strategy

Since today's cybersecurity issues have to be debated at the higher strategic level by organizations, top-management also has to understand the risks their company faces and the possible outcomes of a security event. Yet, corporate managers and cyber experts often talk two separate languages. Citalid aims at closing this gap by collecting data and articulating them into comprehensive and easily intelligible insights. Citalid developed a riskssimulation platform to help managers make the right choices to optimize their cyber strategy fully informed of the risks their business is exposed to.
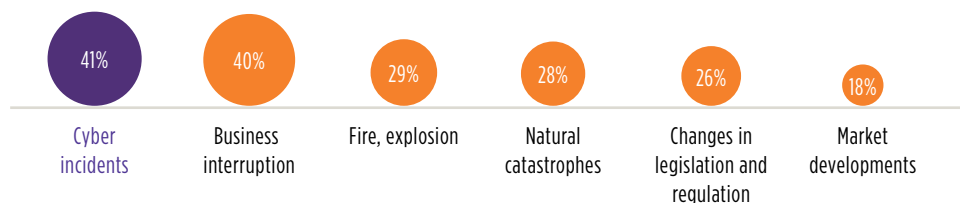
How does it work?

Taking activity domain and geographical presence into account, Citalid first identifies the threats that are the most likely to hit a company. Then using the FAIR methodology to quantify risks, the start-up is able to assess the financial risks businesses are facing. Eventually, investment's strategies and security measures are recommended and adapted as per the maturity of the client.

Ambitious objectives in 2019

Citalid was founded within the operational centre of the French cyber agency ANSSI and has won the 2018 Innovation and Audience Prizes of the awards organized by "Les Assises de la Sécurité". Several French big companies are already using Citalid's platform to quantify their exposure to cyber risks. Willing to become the reference in France when it comes to risk simulation and decision-making support, Citalid is currently raising funds. This should help the start-up accelerate its growth, welcome new recruits and explore other use cases such as the ones on the insurance market.

TOP 6 RISKS IN FRANCE

Cyber incidents	Business interruption	Fire, explosion	Natural catastrophes	Changes in legislation and regulation	Market developments
41%	40%	29%	28%	26%	18%

Source: *Allianz Risk Barometer,* 2019.

Figures represent how often a risk was selected as a percentage of all responses in France.

More than one risk could be selected. Figures don't add up to 100% as up to three risks could be selected.

InCyber

- Created in 2016
- Located in New York (HQ) and Tel Aviv (R&D)
- 3 employees and 8 outsourced engineers
- Field of expertise : True Prediction of Insider Threats (TPIT)

True Prediction to mitigate risks of insider breaches

InCyber is attempting to identify the inside attacker based on the organization log system, which records and documents every activity, account login, balance clarification, or document printing. The start-up developed the first and only solution that predicts insiders threats with nearly zero false positive rate and full compliance with privacy regulations. It was founded by the head of the Israeli R&D Operations, a former police investigator and head of Fraud Prevention at Pelephone, to materialize its previous academic study on the existing means to predict Insider Threat.

InCyber's technology is easy to set up and use

The technology is not based on any predetermined rules but can be used on as many specific tagged activities as wished. Though a low-cost solution, it requires a unique combination of Machine Learning Techniques, Fuzzy Logic, Crowd Sourcing Capabilities and advanced Behavioural Analytics. First, it defines an "Initial Prediction Score" for each user based upon a user activity report and using 5 initial predefined parameters from the company's logs inputs (user ID, date of execution, who executed the action, why, action code). Then, a "Critical Prediction Score" is calculated, applying up to 15 industry factors and using Machine Learning algorithms that learn the business as usual log patterns of a specific monitored activity. Next, the results are correlated with external legal data to maximise the accuracy. At last, the "Crystal Ball Ranking Method™" is used to calculate the "Final Prediction Score", which is reported to the CISO or the CIO.

Azguard

- Created in 2016
- Located in Paris
- 3 employees
- Field of expertise : Identity and Access Management (IAM)

« As users become their own passwords, biometrics is key to secure our digital identities more effectively. »

PATRICE CAINE, Chairman and CEO of Thalès, during the 2019 edition of Viva Technology

Using behavioural metrics to secure authentication

With digital technology continuing to change numerous aspects of our jobs, companies are increasingly exposed to risks. And the battle for digital trust can only be won if technology meets the needs of people while remaining under their control. Therefore, the safety of digital identities has become critical. Using behavioural metrics to authenticate users, Azguard is now able to identify individuals through the analysis of keystrokes patterns describing the movements of users on their keypads. Since the way end users type on the keypad is unique, Azguard is able to prove the identity of the individual accessing a system.

An artificial intelligence to learn from behavioural changes

In addition to behavioural metrics, Azguard is using an artificial intelligence to continuously learn from changes in typing dynamics. Using biometrics and allowing adaptive security by means of an AI, the start-up offers businesses a unique solution to prevent or trace damaging security threats originating from malicious or negligent insiders. Biometrics can help banks or e-commerce companies secure financial transactions and mobile payments, but also industrial groups secure the access to a control-command room or corporates secure the access to the corporate portals, cloud applications, sensitive data and classified files.

nsknox

nsknox

- Created in 2016
- Located in Tel Aviv suburb
- 30 employees
- Field of expertise: Payment Fraud

NsKnox developed TxAuthorityTM to secure every payment

TxAuthorityTM ensures that the right payment order is transferred to the right supplier, with the right account, every time, no matter where the threat comes from (insider or outsider). This is particularly useful for global companies who manage a very high volume of suppliers. It analyses all data at every point in the transaction journey, enabling the detection, alerting, and prevention in real time of fraudulent payment attempts of different types. It allows organizations to define and enforce specific payment policies through external, blind authorities and safeguards payments-run processes, while increasing their Accounts Payable and SOX operational efficiency.

Strong differentiators

Founded by the former Founder & CEO of CyberArk, NsKnox offers the only fully end-to-end protection solution covering both the B2B payment ecosystem and the threats' perimeter, with the data remaining confidential. It uses a Cooperative Cyber Security (CCS) platform shredding data into meaningless pieces of information and storing them in multiple secured locations working in synergy (the "Knoxers") but individually blind to each other's workings by means of "Verifiable Secret Sharing" techniques. These techniques ensure collective efficiency without ever exposing any complete data, and without depending on one single system. It enables verifications to be processed in real time and with high system availability, while making the data storages "zero-knowledge", very hard to hack, manipulate or overwrite. With this easy to test, implement and use solution, NsKnox attracted top-tier corporate investors such as Microsoft Venture Fund, Viola ventures and the Israel Discount Bank.

Payments frauds have grown exponentially

48%
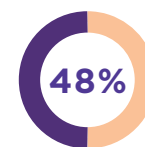
A global survey conducted by PwC among over 7,200 organizations, **revealed that insider fraud players are increasingly active, accounting for 48% of the most disruptive economic crimes experienced today.**

Embedded Solutions

- Created in 2002
- Located in Tel Aviv
- 47 employees
- Field of expertise: Real-time seamless communication protection

ES developed BitNetSentry (BNS) to secure critical activities

Created on the request of ES' clients, BNS is a palm-size network device that may be connected at any network (entry or exit), and that has neither network address nor data link address. Both data rate (Mb/sec) and network behaviour remain unaffected by the system. It allows a seamless and real time reading, understanding and modification of any part of the traffic (context or address). It also avoids forbidden commands (even encrypted and apparently legal ones) and makes 100% sure that your sensitive traffic goes directly from A (inside your company) to B (outside), at a very predictable exact time. BNS is not a standard application level protection. It sits at the lowest level of the network, bringing several key advantages such as independence of the high-level protocols, transparency and the ability to work also with encrypted data. The low-level inspection method can tag and monitor network activity without penetrating or decrypting the data, ensuring client privacy. It also enables bi-directional secured SCADA networking between the user machine interface and the critical infrastructure.

Other key assets

ES' solution was created as a result of the strong experience of collaboration with the army. BNS uses patented "encryption without encryption" abilities and is compliant with privacy regulations. It can be easily and seamlessly integrated in the existing architecture of a company and is certified for avionics and military standards.

WaToo

WaToo

- Created in 2018
- Located in Brest (France)
- 3 employees
- Field of expertise: Data Loss Prevention

Two solutions to prevent data loss

Since data stored by companies have become so vital, protecting databases and files with innovative tools is a necessity. WaToo provides an answer to data leaks and forgeries with two solutions. First, WaTrack protects databases which are made available to partners or sold under license. It identifies the partner or client who leaked or illegally sold data. The second one, WaTwall is integrated into the company's information system to trace daily activity's data. It identifies an unauthorized user who illegally reroutes or leaks data. WaToo solutions do not require any modification of the information system functionalities. WaTrack and WaTwall are patent pending solutions created by academics with more than 10 years of experience in the field of content protection by means of watermarking.
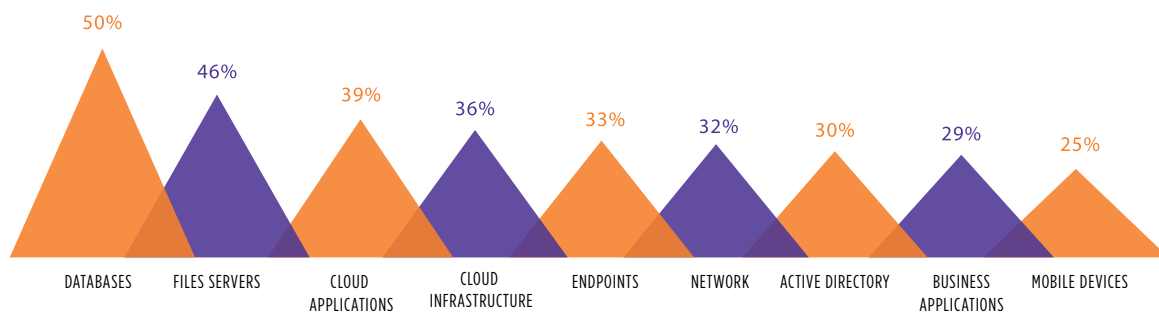
Using watermarking to tag files

The solutions developed by WaToo use tags that are hidden when exporting or accessing the data to ensure its traceability and prevent data loss events. The embedded tags are independent of the information storage format, which means that WaToo's tags remain efficient: a protected Excel file can be exported to CSV and then into a MySQL database, it will still be tagged. Besides, the embedded tags resist most common data modifications: a protected file can be printed and rescanned, it will still be tagged.

These deterrence measures help companies prevent data leaks from insiders or third-parties (partners, subcontractors) and help them to speed up the implementation of corrective counter-measures if a data leak occurs. WaToo's solutions are patent pended.

IT ASSETS AT RISK

Asset	Percentage
DATABASES	50%
FILES SERVERS	46%
CLOUD APPLICATIONS	39%
CLOUD INFRASTRUCTURE	36%
ENDPOINTS	33%
NETWORK	32%
ACTIVE DIRECTORY	30%
BUSINESS APPLICATIONS	29%
MOBILE DEVICES	25%

Source: *Insider Threat Report* by CA Technologie, 2018.
Cybercriminals see a greater opportunity in targeting where data is located in volume.

Jean-Claude Laroche

Jean-Claude Laroche is the Chief Information Officer of ENEDIS and preside the Cybersecurity Circle of the Cigref, a network for large companies promoting "Digital Culture as a source of innovation and performance". He is the former CIO of EDF, the largest European electric utility, and worked as a member of the Board of Directors of the European Cybersecurity Organisation (ESCO). In this interview, Jean-Claude Laroche details both the main challenges large companies have to overcome to secure their assets and the conditions for an effective collaboration between small and medium-sized companies and global organizations.

WHAT ARE THE NEXT CHALLENGES BIG COMPANIES AND GOVERNMENTS WILL HAVE TO OVERCOME IN THE NEXT FEW YEARS?

The first challenge is related to the intensification and complexification of malicious security breaches on Information Systems. This is also a consequence of the increasing involvement of governments in cybersecurity programmes, including offensive programmes. Hence the necessity for most companies to catch-up and upgrade their processes to match the surging threat. Today, they have to clarify their governance, to overhaul their defensive doctrine, to plan response and to develop skills - and a lot is at stake with this last issue. Most important is the fact that big companies have to embrace the cybersecurity issues at the higher management level. For the current risks do not only have an impact on information systems, but on the global companies' operations.

TAKING THIS CONTEXT INTO ACCOUNT, WHAT DO YOU EXPECT OF INNOVATIVE START-UPS DESIGNING CYBERSECURITY SOLUTIONS?

The one thing I witness is that innovation exists on the offensive side. Therefore, if we stand still and don't enhance our defensive capabilities, sooner or later will we be overwhelmed and overpowered by aggressors. I consequently see a great interest in discovering innovative defensive solutions when they are developed by people knowing the attackers mindset. This allows us to keep up the pace with the rising threats. Since it can yield evolution …

AND WHAT SPECIFIC ROLE CAN START-UPS PLAY TO CREATE THIS MUCH NEEDED INNOVATION?

For me, innovative start-ups are of great interest for sure. Yet, it is not always to build business relationships. Start-ups first have to go through the challenge of their sustainability, before going into partnerships with big companies seeking continuity. Sometimes, the most interesting part of a start-up is the expertise of its staff members. Immersion in the cybersecurity domain often give them a comprehensive knowledge of what a cyberattack really is. This gives them a competitive edge to design solutions.

THE MAIN TOPIC OF OUR WATCH IS "INSIDER THREAT". WHAT ARE THE MEASURES A BIG COMPANY LIKE ENEDIS IS IMPLEMENTING TO PREVENT INSIDER EVENTS?

This topic is extremely delicate. Actually, "Insider Threat" refers to a more important issue: digital trust. For there won't be a sustainable digital transformation without trust in the new processes involved. There are two types of insider threats: unintentional ones and malicious ones. Unintentional threats are mostly caused by a lack of awareness or a lack of skills. Since these unintentional events are the most likely to occur, preventing them must

be a top priority for companies. The lack of skill I evoked is at the root of the first insider threat. Thus, tackling this issue is mandatory and should become a top priority. Part of the solution reside in awareness and recruitment. Yet, awareness is a continuous task and recruitment is harsh today as knowledge remains hard to find. Regarding malicious insiders willing to harm the company, knowledge is key to mitigate risks. Especially when it comes to critical assets, companies have to do their best to know collaborators joining the staff. Yet, zero-risk does not exist. Simultaneously, measures are deployed to monitor the information system and detect irregular patterns or frauds. Today, audit and surveillance capabilities are a must for companies, as well as specific process for crisis management.

WHAT WOULD BE THE MAIN BENEFITS FOR A LARGE FRENCH COMPANY TO BUILD COOPERATION PROGRAMMES WITH ISRAEL IN CYBERSECURITY?

I had the opportunity to get a close look to the specificities of Israel in cybersecurity. Since cyber defense has entered in the range of Israel's national strategic interests, the country made sure to have human skills available. The education system and the national service has helped to build a unique dynamic. Therefore, cybersecurity ideas and initiatives exist that could help us change the way we secure our systems and make indisputable progress.

The crux of the issue lies in the ability for start-ups, especially early-stage start-ups to overcome the challenge of sustainability and to accept long sales cycles to work with a large company like ENEDIS. There is a gap in pace between our processes and start-ups' processes.

Professor Isaac Ben-Israel

Major General Professor Isaac Ben Israel is called "the father of Israeli cybersecurity". Working at the Tel Aviv University, he is also the Chairman of the Israel Space Agency and of the Israel National Council for R&D. He won several prestigious awards such as the IDF Director of military intelligence Prize for Creative Thinking in 1984 and the Lions "Man of Excellence" for his contribution to Israel's Security in 2008. In this first part, Pr. Isaac Ben Israel reveals the origins of the Israeli state strategy in the cyber domain. In the next release of our Watch, the second part of this interview shall be released to explicit Pr. Ben Israel's view on innovation and cooperation in cybersecurity.

IN 2010 YOU WERE APPOINTED BY THE ISRAELI PRIME MINISTER (PM) TO LEAD A TASK FORCE THAT FORMULATED ISRAEL NATIONAL CYBER SECURITY POLICY. IN 2015, YOU RECOMMENDED TO THE PM THE CREATION OF THE NATIONAL CYBER AUTHORITY. WHAT WERE THE STRATEGIC THOUGHTS BEHIND THESE RECOMMENDATIONS?

Let me come back to the year 1998. In 1998, this was after a few years of experience in IDF (Israeli Defence Forces), I was the Head of Research & Development (R&D) at the Ministry of Defence's Directorate. I wrote a letter to the Israeli PM (Ehud Barak), in which I told him: "One day, everyone will understand the potential of Cyber Security (CS) as a weapon. As long as we know it, but our enemies don't, we have an advantage over them. But the day everyone will know it, then we will have a weakness, because in Israel, everything is controlled by computers, especially our critical infrastructures. Therefore, we'd rather start preparing ourselves to it".

Following this, in 2002 (I was still at the same position), the government created a new unit in the Shabak (Interior Security services) in charge of cyber protection of critical infrastructures, i.e power production, water supply, transportation… But until the end of the decade, it was a secret. Other countries, including France, did the same (under military and intelligence organisations), but it was not publicly known capabilities. Until the attack on the Iranian centrifuges was exposed in 2010. No one knows for sure who did it, although the media usually attributes it to Israel.

At this moment, the Israeli PM called me and said: "You remember the letter you wrote in 1998? This is happening, we are there", because this event caught the attention of the global media and people of different horizons started to think about the cyberattacks' possibilities. Indeed, these centrifuges were destroyed without shooting any bullet, or putting a bomb. The PM said to me: "This is the day, I will appoint you to lead a taskforce and it is simple: You'll start by predicting the treats, then thinking about possible solutions, then prioritize them, and finish with a 5 years plan to prevent them".

And I answered him: "It cannot be done! Not by us, nor by anyone. Because, the rate of change of CS technology is in fact so fast, that no one can predict what will be the threats 5 years from now. We have a new generation of technology about every 1.5 years, so 5 years represents more than 3 generations away. It may happen that next week, someone will come with a new CS idea and we will find it in the field a year later. And until we finish the report that you require, it will be already obsolete. The only thing that we can do is build a system that will know what to do once these unpredicted threats will appear".

WHAT WERE THE ELEMENTS OF THIS SYSTEM?

The first most important component is knowledgeable people. We had to change our education system. At that time, there was not even one university in the world in which you could earn a degree in CS. So, we had to teach CS in high schools, as the students entering universities come from there. And that's how, until today, Israel is the only country in the world where we teach CS in high schools and today, even in elementary schools. To young children, we don't teach them to write CS codes, but we teach them how to behave in the CS world. It's like for a driving licence. We give kids a licence to drive only when they are 17 years old but from the age of 5, we teach them how to live in this world. But in high school, we teach them coding. Alike, we also recommended that every university will have CS Research, because practitioners in Defence and Intelligence were not interested in solving basic problems and the only way to do so was through academic research.

Then we had the problem of industry. If you want a solid ecosystem, it is not enough to have knowledgeable people that will know what to do when the unexpected and unpredictable threats will emerge, because in such case, we don't have much time to solve it. So, the idea was to have actors that are ready to pick up any problem and quickly tailor a specific solution and make it available to the market. This led us to the idea of having a lot of start-ups starting to play with new ideas, even if it's not fully cooked, to enable the people to find the right solutions quickly. But in Israel, start-ups are usually built from bottom up, meaning kids after the military service come with ideas that they want to concretize. How could we give them motivation to do it in CS as in other areas? Adding to that, start-ups need investment. That's why, we thought that we

needed a self-sufficient, self-contained and self-maintained industry, to finance the start-ups development and patch the IP through exit.

On top of it, CS is a kind of dual weapon, because you may develop it to defend yourself but if it falls in the wrong hands, someone may use it against yourself. When exporting or selling physical weapons, you can require from the companies to ask for export licences from the government, to avoid that these weapons will fall in the wrong hands. However, traditional weapons are usually developed and produced by very big defence companies. In CS, you speak of small groups of people (sometimes quite young) from whom you can't require this because they don't have the resources (time, money, people...) for such negotiations.

It was a problem because in Israel, every industry heavily relies on export, given the fact that the local market is always too small. So, we decided to not compel any defensive CS start-ups to require a governmental licence approval. Only, the offensive CS start-ups should go to the government.

So, we found ourselves having to think a whole complete ecosystem: Education, Start-ups, Industry, different Government entities. On the other hand, fortunately, we didn't have to reinvent the wheel because we already had a strong high-tech ecosystem, including disciplines that are more or less the same as in CS: Computers, Communication, Microelectronics, Software... So, we just had to find the mechanism that will give incentives to all these high-tech ecosystem's players to shift to CS. This is what we did,

and it worked. This plan was submitted to the government in 2011 and started to be implemented from January 2012.

By the end of 2013, the Snowden affair was revealed, and we learned from it that there is strong internal tension between, Privacy and Human Rights for democracies' citizens on one hand, and on the other hand, Security. So, we aimed at concretely minimize this tension and this is what led us to eventually (as of January 2015) set up this new Cyber Defence authority in charge of defending the civilian cyberspace, that we merged with the already existing Shabak entity.

To be continued...
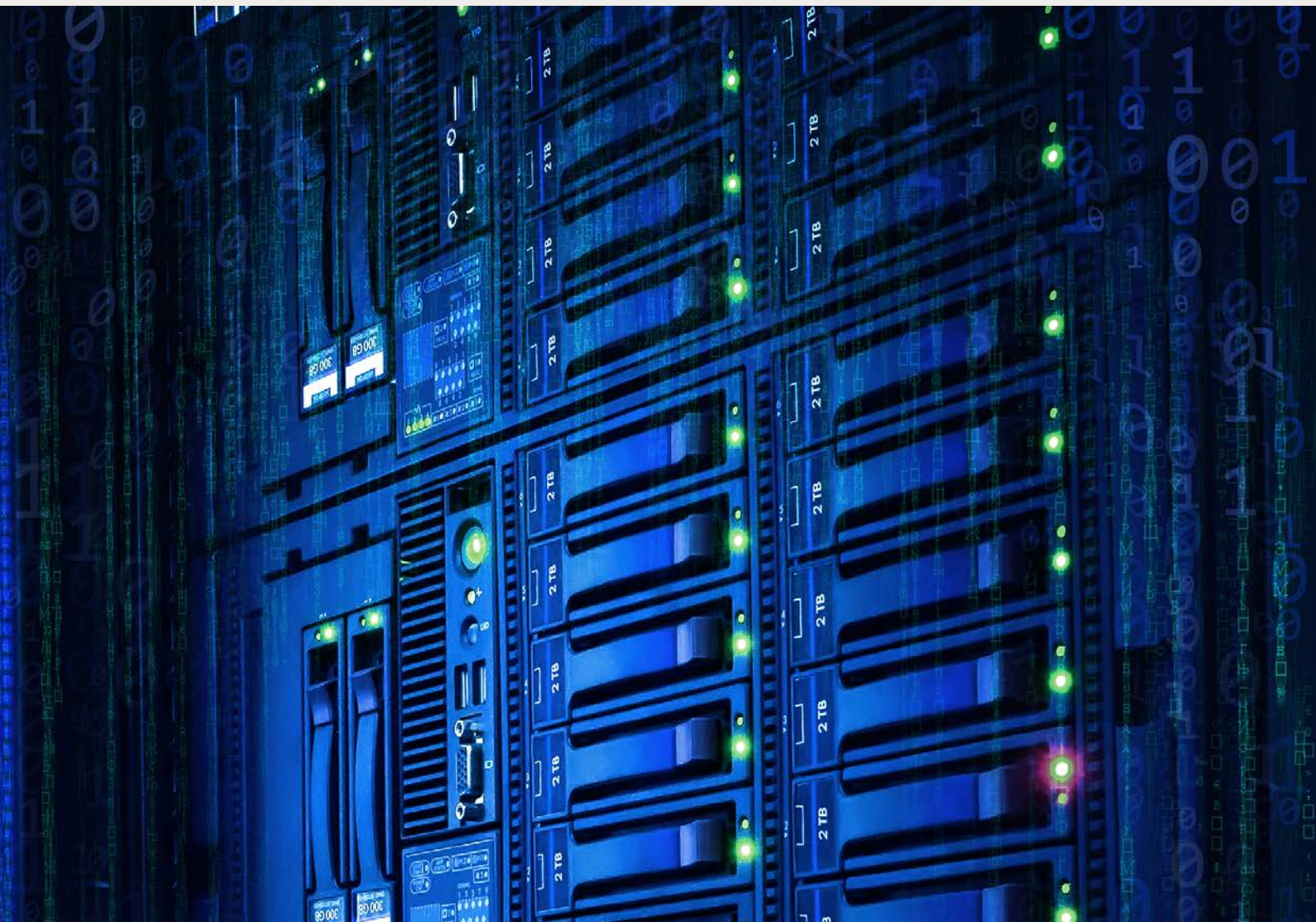
Israeli and French cybersecurity start-ups to watch in 2019

ReachFive

- Created in 2014
- Located in Paris
- 25 employees
- Field of expertise: Customer IAM

Customer Identity solutions

ReachFive provides Customer Identity and Access Management (CIAM) solutions allowing companies to use an integrated and unified SaaS platform to create a unique user experience. These are omnichannel solutions working with a multi-cloud platform aiming at creating disruptive customer-centric experiences. Authenticating users, collecting consent and accurate data, the platform can build customer profiles and offer its clients the possibility to ask direct questions to the end-customers. Organizations can consequently leverage valuable insights to personalize marketing.

Acquiring customers' insights with ease

ReachFive is already designing the authentication solutions for dozens of e-commerce websites or applications in 55 countries, including Etam Group, Engie, Monoprix, Boulanger, L'Occitane, Saint Gobain, Lacoste, and La Redoute among many others. Its platform does not simply store emails and passwords. It shares information through different channels (websites and physical stores for example) seamlessly for the customers, while being fully compliant with the GDPR. ReachFive also supports social logins, such as Facebook Connect, and can be integrated with other software, such as a CRM.

New European ambitions

Managing over 40 million customer accounts, the start-up founded in 2014 by Jérémy Dallois, has strong growth objectives. Willing to double its staff and to commercialise its platform in Germany and in the UK, ReachFive has raised $10 million in April in a series A funding led by CapHorn Invest and involving Ventech and Dawn Capital (a London-based VC firm).

KINDITE

Kindite

- Created in 2017
- Located in Tel Aviv
- 15 employees
- Field of expertise: End to end solution for database encryption

The next generation of encryption

Enterprises look into the cloud with frustration. They are interested in taking advantage of the cloud's flexibility, cost savings and simplicity but by moving to the cloud, organizations willingly handle their data to a third-party entity, meaning data is exposed in that remote environment, out of their controlled domain. How organizations can enjoy the benefits of cloud environments without losing control over their data? These are the precise critical hurdles Kindite helps to overcome with a disruptive solution using several patent-pending cryptographic technologies.

Searchable Encryption to secure cloud adoption

Kindite was founded to make sure encryption keys never leave the organization's domain while performing end-to-end encryption of data at rest, in transit and most importantly, in use. Their "Zero-trust Encryption" technology enables processing encrypted data within the cloud environment and decrypting it at the end-point only. This eliminates the necessity to compute over plain-text data at the cloud and assures sensitive data is truly protected. Kindite's service can be seamlessly integrated with each of the enterprise applications stack without any noticeable latency nor harm to application functionality. In other words, Kindite breaks the long-lasting trade-off of data security/privacy and cloud functionality, truly opening the cloud for mass adoption of security savvy and regulated organizations

Sqreen

- Created in 2015
- Located in Paris and San Francisco
- 35 employees
- Field of expertise: Application Security

Helping businesses monitor their applications

Sqreen is a French cybersecurity start-up that helps security and engineering teams monitor and protect web applications from vulnerabilities and attacks (including SQL injections, cross-site scripting, broken authentification and other common attacks recorded by the OWASP). Its application security management platform uses "microagents" into applications that identify and fight threats, providing businesses with real-time insights and blocking infiltration attempts.

Reinventing the way web applications are secured

Aiming to simplify security on the Internet, Sqreen's unique selling point is the ease of deployment of its solution. The solution works with web applications, APIs or microservices using most programming languages and can be deployed on any cloud, hybrid or on-premise architecture. Developers just have to install a library on the servers to take advantage of the reports of Sqreen. They also benefit from optional real-time protection modules to help secure the applications like Runtime application self-protection (RASP), an in-app Web Application Firewall (WAF), protections against account takeovers or bad bots, etc.

$14 million raised to accelerate commercialisation

Founded by CEO Pierre Betouin and CTO Jean-Baptiste Aviat who both worked at the Apple Red Team, Sqreen is headquarted in Paris and San Francisco. Already helping to secure the applications of over 500 companies including LeMonde, BlaBlaCar or Algolia, the company has raised $14 million in Series A funding in April, mostly to expand the sales effort on the American market. Greylock Partners, one of the oldest and most iconic venture capital firms led the funding round.

Segasec

- Created in 2017
- Located in Tel Aviv
- 20+ employees
- Field of expertise: Brand Identity Abuses' Protection

Protect your brand identity from digital abuse

Segasec breakthrough technology enables unbeatable early and undetectable detection, especially to uncover hidden/masked digital impersonation. It allows company to prevent abuses such as phishing sites, false domains or content replication. The start-up developed the first solution offering impersonators' "strike back deception" services, as well as an unprecedented level of Cyber Intelligence & Response services. It doesn't require integration as it is a zero on-boarding product. This means CISOs can start using the service within minutes.

An "all in one" solution

Experiencing a very fast and organic growth, Segasec offers a solution enabling both detection and response. First, it ensures a patent-pending "24x7 Intelligence" performing quadrillions of scans, utilizing past data and machine learning algorithms, and a patent-pending "Proactive non-domain detection" with undetectable, easy-to-install web agent uncovering mimicked site content. Then, it operates a response with lightning-fast automation of block-and-take-down. The deception mechanisms manipulate and confuse the attackers, making their data unusable. Segasec uses the best of AI & ML technologies to ensure tailored detection and intelligence.

Israel: Discover the CESIN's Learning Expedition

Organized by the CESIN (the Information and Digital Security Experts' Club) in collaboration with CEIS, Wavestone and Shushane & Co, and sponsored by Palo Alto, the 2019 edition of the Learning Expedition will be hold from Saturday 22nd to Wednesday 26th June 2019 at the occasion of the Tel Aviv Cyber Week. It aims at helping CISOs and cybersecurity professionals to find concrete answers to their day-to-day challenges. It is also a unique opportunity to discover the latest innovation trends in Israel and exchange with the prominent actors of the Israeli cybersecurity ecosystem, such as CISOs, start-ups, investors, public French and Israeli organisations, R&D centres, NGO, etc.

A rich programme

Key moments of this Learning Expedition include, among others, the visits of Beer Sheva's CyberSpark (the heart and soul of innovation in cybersecurity where major actors gather), of the national CERT, of the SOC of a critical Israeli operator, of the cyber R&D center of a global company, and meetings with a prominent VC, with the Israeli Innovation Authority, with the French Embassy, with the Cyber Directorate and with key players in cyber education. Delegates will also attend the Tel Aviv Cyber Week, one of the largest annual international cybersecurity events.

Notable funding rounds in Israel in 2019

Month	Company	Date of creation	Field of expertise	Amount raised (in million of US dollars)	Round
February	**nsKnox**	2016	Payment fraud	15	A
	Axonius Inc.	2017	Cybersecurity asset management (CSAM) service	13	A
	Firedome Inc.	2018	Endpoint detection and response cybersecurity for smart-home devices.	4,5	A
	C2A Security	2016	Cars' internal systems protection against cyberattacks	6,5	A
	PerimeterX	2014	Protection against automated bot attacks	43	C
March	**CyberX**	2013	IIOT & ICS, cybersecurity	18	B
	Cymulate	2016	Breach and attack simulation platform	7,5	A
	Sayata Labs	2016	Cybersecurity risks analysis for small and medium-sized companies	6,5	Seed
	Perimeter 81	2013	Cloud-based software defined perimeter	5	A
May	**Veego**	2019	Elimination of IoT and connected home devices' malfunctions	5	Seed
	Hunters.AI	2018	First automated threat hunting solution	5,4	Seed

Notable exits in Israel in 2019

Month	Company	Date of creation	Field of expertise	Amount raised (in million of US dollars)
February	**Palo Alto Networks**	2016	Security Orchestration, Automation, and Response (SOAR) platform	560
	Luminate Security	2017	Zero-Trust Application Access	around 200
May	**Meta Networks**	2016	Breach and attack simulation platform	120

Event recap

2019 cybersecurity innovation awards in France

Precisely aiming at bringing support to French cybersecurity start-ups and identifying the next French and European gems, innovation awards are once again flourishing in 2019 in France. Next July, Société Générale and Wavestone will announce the winners of its Banking CyberSecurity Innovation Awards (BCSIA). Among many others, this year's prestigious jury includes Guillaume Poupard (Director General of ANSSI), Claire Calmejane (Innovation Director of Société Générale) and Pascal Imbert (CEO of Wavestone).

Almost simultaneously, the awards' winners of the 2019 edition of the Innovation Prize of the "Security Assises" will be announced after having successfully presented their solutions to 400 cybersecurity professionals

The 2019 French Cybersecurity Start-ups Radar released during Viva Technology

From Thursday 16th to Saturday 18th May, Wavestone attended the 2019 edition of Viva Technology, the world's rendezvous for start-ups and leaders to celebrate innovation and tomorrow's possibilities in Paris. Besides Wavestone's presence as a sponsor of the

Media Lounge and of the Press Center, the event gave Wavestone the opportunity to host international delegations, attend conferences' tracks on hot topics such as "Future technologies" and introduce some of its latest releases. Viva Technology offered Wavestone a unique stage to reveal its 2019 edition of the "French Cybersecurity Start-up Radar", assessing the current dynamics and challenges start-ups face.

The reports depicts a fast evolving start-ups landscape and today's dynamics helping start-ups perform.

Learn more on Wavestone's blog RiskInsight.

France: A booming funding environment

More funding rounds and more capital driving momentum in France

The overall French start-up landscape is booming, and private investment is clearly playing its role of catalyst for many start-ups. In 2018, 645 French start-ups raised funds (40% year on year increase) for a total of 3.6 billion euros. The surging number of funding rounds is also happening for cybersecurity start-ups. Since June 2018, 18 French cybersecurity start-ups have raised more than 1 million euros, led by Alsid and Sqreen, who have respectively raised 13 and 12 million euros last April, or CyberlAngel, Sentryo and Odaseva, each of them having raised 10 million euros in the previous months. Furthermore, 27% of the French cybersecurity start-ups interrogated by Wavestone (over 100 start-ups) declared being currently raising funds, proving that the hype of buzzing venture capitalists and private investors eventually hit cybersecurity.

Supported by this dynamic, the French start-up ecosystem seems to experience a period that is ripe for innovation in cybersecurity. The adoption of new regulations compelling companies to adopt ambitious compliance programmes, such as the GDPR or the LPM for critical national operators, have acted as major wake-up calls. It has also created a wide array of opportunities for start-ups to benefit from. On the eve of scaling up, the French cybersecurity start-ups ecosystem requires continuous efforts to support innovation.

France: A booming funding environment

100M€

HAS BEEN RAISED IN SEED OR SERIES A FUNDING SINCE JUNE

Company	Description
ALSID	French Active Directory breaches prevention company raised $14.5M in April 2019
sqreen	Application security management platform start-up raised $14M in April 2019 as part of a Series A funding round led by Greylock Ventures
odaseva Backup - Archive - GDPR	The start-up providing a full suite of data management raised $11.7M in February 2019
sentryo	Founders of the security platform dedicated to ICS and IoT raised $11.2M in December 2018
CybelAngel	Digital risk management platform start-up completed a second round, raising $11.2M in October 2018
reachfive	Customer identity solutions pure play raised $10M in April 2019 to accelerate commercialisation across Europe
ACORUS NETWORKS	The start-up offering a DDoS protection for both network and application layers raised $5.6M in April 2019
YESWEH4CK European Bug Bounty Platform & Infosec Jobs	Leading European Bug Bounty platform YesWeHack raised $4.5M in February 2019

How did we build the first issue of the "France – Israel Cyber Innovation Watch"?

Shushane & Co and Wavestone seized the opportunity to join forces and deliver a new publication aiming to capture in a comprehensive way the France's and Israel's cybersecurity innovation landscape. As cybersecurity remains a fast-evolving sector in which innovation plays a critical role, this "Innovation Watch" was also designed to introduce some carefully selected French and Israeli start-ups providing disruptive powerful solutions to address today's most critical cybersecurity challenges, while helping readers to understand the key value proposition, unique selling points and other differentiating assets of these start-ups.

How to enjoy the "France-Israel Cyber Innovation Watch" publications?

This "France – Israel Cyber Watch" will be published every 4 months. If you are a CIO, a CISO, a Risk Manager, an investor and want to be informed of our next release or a French or Israeli start-up willing to be cited, please contact us.

To suscribe to the content and discover the Cyber Innovation Watch's membership fee, please contact Wavestone at the following address:

CyberInnovationWatch@wavestone.com

Shushane & co

www.shushaneandco.com

Shushane & Co is a company based in Tel Aviv, specialised in Business Breakthrough Innovation. Its offer is twofold and includes:

1 – Tailored initiatives to develop international cooperation with Israel in innovation, particularly in cybersecurity, security and IT, and including learning trips, technological watch and strategic partnerships' follow through

2 – Companies' management coaching to foster internal and external innovation programmes

WAVESTONE

www.wavestone.com

In a world where knowing how to drive transformation is the key to success, Wavestone's mission is to inform and guide large companies and organizations in their most critical transformations, with the ambition of a positive outcome for all stakeholders.